# Incident Tracking, Event Management and Threat Analysis: Operational Applications for Automation Protocols

Tom Millar, US-CERT

# ITAP: User Stories

- We have to process hundreds of incident reports a day
- We have to make rapid decisions to prioritize, escalate and respond
- We need to automate as much of the data entry work as possible
- We need the results to be structured to enable knowledge discovery and show real changes over time

# ITAP: What If ?

- …We wrap CEE log files in a reporting schema like IODEF?
- Along with MAEC-formatted malware metadata?
- …We start associating CAPEC and CWE references to help find root cause?
- What about a “Common Severity Scoring System” for Incident Impact Assessments?
- Think real-time decision assistance for triage

# EMAP User Stories

- We have to process billions of system and network events a day
- We have to cut sort awk and grep
- We need to speed up the OODA loop(s) from detection to mitigation
- We need to share anonymized event patterns with our partners for collaborative investigation and situational awareness

# EMAP: What If ?

- …We leverage something like FLAIM for CEE to enable quick traffic and log sharing?
- …We “tag” sets of events with related CAPEC or MAEC characteristics?
- …We tie OVAL and XCCDF checks to identified event patterns to quickly surmise the most important state features of potential targets?

# TAAP User Stories

- We have to track dozens of “threat families”
- We have to produce dozens of warning docs and use homemade scripts to keep up with changing tactics
- We need to find relationships between hundreds of indicators of different types
- We need to keep up with dozens of semi-structured tips (blogs, e-mail, atom/rss feeds, watchlists) across multiple environments

# TAAP: What If ?

- …We could “tag” certain MAEC elements and quickly document relationships?
- …We could wrap recommended XCCDF or OCIL in incident notifications and warning reports?
- …We could employ handling standards like Traffic Light Protocol or CAPCO across threat report elements to enable quick “tearline” versions and faster knowledge sharing?

# Thinking like an operator

- Structured data is only as good as the decision it helps you make
- This is Knowledge Management with an eye to improving process performance
- Mapping data elements to a Net Defense OODA is not just an exercise
- *Smarter*, better, faster, stronger (not harder)

Tom Millar, US-CERT

Usually:

thomas.millar@us-cert.gov

And/or:

thomas.millar@dhs.gov